Discrete Mathematics 28 (1979) 315–319

HOW MANY WAYS CAN A PERMUTATION BE FACTORED INTO TWO n-CYCLES?

David W. WALKUP*

Department of Computer Science, Washington University, St. Louis, MO 63130, USA

Received 22 February 1978
Revised 6 November 1978

A recursion is developed for the number $f(P)$ of ways a permutation P on n symbols can be written as a product of two n-cycles. It is known that $f(P)>0$ if and only if P is an even permutation. It is shown here that $f(P)/(n-1)!=f(Q)/(m-1)!$ if P has trivial cycles but the same nontrivial cycle structure as a permutation Q on m symbols, while $1\leq f(P)/(n-2)!\leq\frac{7}{3}$ if P is even and has no trivial cycles. Additional evidence strongly suggests $f(P_n)/(n-2)!\to 2$ as $n\to\infty$ for any sequence of even P_n on n symbols without trivial cycles. Some connections with Hamiltonian cycles in a random graph and the group structure of the symmetric group are noted.

1. Introduction

Let $f(P)$ denote the number of ways a member P of the group S_n of permutations on n symbols can be written as the product of two cycles of length n. Obviously $f(P)$ depends only on the cycle structure of P, and it is known that $f(P)>0$ if and only if P is a member of the alternating subgroup A_n, that is, if and only if P can be written as the product of evenly many transpositions. As Theorem 1 below shows, $f(P)$ depends to a large extent only on n, the number of symbols actually moved by P, and the evenness of P. The formulas for $f(P)$ given in Table 1 are representative of a fairly complex recursion explained in Section 2 and used in Section 3 to prove Theorem 1.

Theorem 1. *If $P\in S_n$ and $Q\in S_m$ have the same nontrivial cycle structure, then*

$$f(P)/(n-1)!=f(Q)/(m-1)!.$$

If $P\in A_n$ and P has no trivial cycles, then

$$1\leq f(P)/(n-2)!\leq\tfrac{7}{3}.$$

A proof of $f(P)>0\Leftrightarrow P\in A_n$ due to Gleason is reported in [3]. This is just one of a variety of similar results on existence of factorizations in finite and infinite permutation groups to appear since the basic paper by Ore [5] in 1951. Some more recent papers are those by Bertram [1], Moran [4], and Brenner and Riddell [2].

* Now with Aerospace Corporation, P.O. Box 92957, Los Angeles, CA 90009, USA.

Despite more than a surface connection with Gleason's proposition, Theorem 1 actually arose independently in an investigation of Hamiltonian cycles in very sparse random directed graphs using ideas from [7] and [8]. In [8] Wright shows $|K_n| \sim (n-1)!\,e^{-1}$, where K_n is the set of Hamiltonian cycles V arc-disjoint from a canonical cycle U in a complete directed graph on n nodes. By interpreting U and V in the obvious way as permutations in C_n and considering $P = U^{-1}V$, it can be seen that

$$\sum_{P \in D_n} f(P) = (n-1)!\,|K_n|,$$

where D_n is the set of fixed-point-free (or deranging) permutations from S_n. $|D_n|$ is well-known as the Euler rencontre number. A trivial modification of the standard inclusion-exclusion proof [6] of $|D_n| \sim n!\,e^{-1}$ using $|A_n| = \frac{1}{2}|S_n|$, $n \geq 2$, will prove $|A_n \cap D_n| \sim \frac{1}{2}n!\,e^{-1}$. Thus, the asymptotic average value of $f(P)/(n-2)!$ for $P \in A_n \cap D_n$ is 2. Theorem 1 and averaging tendencies of the recursion for $f(P)$ given in Section 2 suggest the following:

Conjecture. $f(P_n)/(n-2)! \to 2$ as $n \to \infty$ for any sequence of P_n, $P_n \in A_n \cap D_n$.

2. Recursion for $f(P)$

Let S_n be realized as the group of permutations on the symbols $\{1, 2, \ldots, n\}$ with *products and operators composed left to right* and denote by C_n the subset of $(n-1)!$ permutations which are n-cycles. Obviously, $f(P) = |F(P)|$ where

$$F(P) = \{(U, V) \mid P = UV,\ U \in C_n,\ V \in C_n\}$$

for any $P \in S_n$. For $1 \leq i \leq n$ define operators $\phi_i : S_n \to S_{n-1}$ by

$$P\phi_i = [P(nP, i)(i, n)]\pi_n^{-1},$$

where (nP, i) denotes the permutation which transposes i with nP and π_n is the natural embedding of S_{n-1} in S_n. Note that

$$P\phi_i = P\phi_n = [P(nP, n)]\pi_n^{-1}$$

whenever (n, i, nP) are not all distinct (and not just when $i = n$).

The algebraic definitions of ϕ_i and ϕ_n above are used in proving Lemma 2 and the basic recursion on $f(P)$ given in Theorem 2. Lemma 2 may be viewed as a much expanded enumerative version of Gleason's existence proposition [3]. Lemma 1 gives an alternate graphical interpretation of ϕ_i and ϕ_n in terms of the cycle structures of the permutations involved.

Theorem 2. $f(P) = \sum_{n \neq i \neq nP} f(P\phi_i)$.

Lemma 1. *The cycle structure of $P\phi_i$ may be obtained from P by one of the following:*

(a) *If* $nP = n$, *the trivial cycle on* n *is deleted.*

(b) *If* $i = nP \neq n$ *or* $i = n \neq nP$, *the cycle* $c(n, P)$ *containing* n *is replaced by a (possibly trivial) cycle of length* $|c(n, P)| - 1$.

(c) *If* (n, i, nP) *are distinct and* $i \notin c(n, P)$, *the cycles* $c(n, P)$ *and* $c(i, P)$ *are replaced by a nontrivial cycle of length* $|c(n, P)| + |c(i, P)| - 1$.

(d) *If* (n, i, nP) *are distinct and* $i \in c(n, P)$ *with* $i = nP^k$, $2 \leq k \leq |c(n, P)| - 1$, *then* $c(n, P)$ *is replaced by two (possibly trivial) cycles of length* $k - 1$ *and* $|c(n, P)| - k$.

Lemma 2. *For* $1 \leq i \leq n$, *put* $S_{n,i} = \{P \in S_n \mid nP = i\}$, $C_{n,i} = S_{n,i} \cap C_n$, *and* $F_i(P) = F(P) \cap (C_n \times C_{n,i})$.

(e) $S_n = \bigcup_i^+ S_{n,i}$, $C_n = \bigcup_{i \neq n}^+ C_{n,i}$, *and* $F(P) = \bigcup_{n \neq i \neq nP}^+ F_i(P)$, *where* $\bigcup^+$ *signifies disjoint union.*

(f) *For all* i *and* j, ϕ_i *induces a bijection of* $S_{n,j}$ *onto* S_{n-1} *with inverse given by* $P'\phi_{i,j}^* = P'\pi_n(n, i)(i, j)$.

(g) *For* $j \neq n$, ϕ_n *induces a bijection of* $C_{n,j}$ *onto* C_{n-1} *with inverse* $\phi_{n,j}^*$.

(h) *For* $n \neq i \neq nP$, *the map* $\Phi : S_n^2 \to S_{n-1}^2$ *given by* $(U, V)\Phi = (U\phi_n, V\phi_n)$ *induces a bijection of* $F_i(P)$ *onto* $F(P\phi_i)$ *with inverse given by* $(U', V')\Phi_{i,nP}^* = (U'\phi_{n,k}^*, V'\phi_{n,i}^*)$, *where* $k = nP(V'\phi_{n,i}^*)^{-1}$.

Proofs. Theorem 2 is an elementary consequence of (e) and (h) of Lemma 2. Lemma 1 is easily checked by visualizing P and $P\phi_i$ as directed graphs. In particular, $P\phi_i$ is obtained from P in (c) and (d) by deleting n and its incident arcs, adding an arc from nP^{-1} to nP, and then switching the destination of this arc with that of the arc from iP^{-1} to i. Part (e) of Lemma 2 is obvious. (The terms for $i = n$ and $i = nP$ omitted from the formula for $F(P)$ correspond to impossible conditions $nV = n$ and $nU = n$.) To prove (f) it suffices to check first that ϕ_i and $\phi_{i,j}^*$ do indeed send $S_{n,j}$ and S_{n-1} into each other and then verify algebraically that their composition in either order is an identity. Part (g) is derived from (f) by verifying (using reasoning as in (b)) that ϕ_n and $\phi_{n,j}^*$ send $C_{n,j}$ and C_{n-1} into each other. The proof of (h) is similar. Thus, the computation

$$\begin{aligned}(U\phi_n)(V\phi_n) &= [U(n, nU)V(n, nV)]\pi_n^{-1} \\ &= UV(nV, nUV)(n, nV)\pi_n^{-1} = (UV)\phi_{nV}\end{aligned}$$

together with (g) shows $\Phi : F_i(P) \to F(P\phi_i)$. Similarly,

$$\begin{aligned}(U'\phi_{n,k}^*)(V'\phi_{n,i}^*) &= U'\pi_n(n, k)(V'\phi_{n,i}^*) \\ &= U'\pi_n(V'\phi_{n,i}^*)(i, nP) \\ &= (U'V')\pi_n(n, i)(i, nP) = (U'V')\phi_{i,nP}^*\end{aligned}$$

shows $\Phi_{i,nP}^* : F(P\phi_i) \to F_i(P)$. Part (g) shows directly that three of the four compositions of the components of Φ and $\Phi_{i,nP}^*$ are identities. The fourth identity, $U\phi_n\phi_{n,k}^* = U(nU, n)(n, k) = U$, follows from $nU = nPV^{-1} = nP(V\phi_n\phi_{n,i}^*)^{-1} = k$.

Table 1

P	n	$f(P)$	$f(P)/(n-2)!$	formula for $f_n(P) \equiv f(P)$
$P_1 = (1)$	1	1	—	—
$P_2 = (3, 2, 1)$	3	1	1.0	$f_1(P_1)$
$P_3 = (4, 3)(1, 2)$	4	2	1.0	$2 \cdot f_3(P_2)$
$P_4 = (5, 4, 1, 2, 3)$	5	8	1.333	$2 \cdot 3 \cdot f_3(P_2) + f_4(P_3)$
$P_5 = (6, 5)(1, 2, 3, 4)$	6	32	1.333	$4 \cdot f_5(P_4)$
$P_6 = (6, 5, 1)(2, 3, 4)$		36	1.5	$4 \cdot 3 \cdot f_3(P_2) + 3 \cdot f_5(P_4)$
$P_7 = (7, 6, 1, 2, 3, 4, 5)$	7	180	1.5	$2 \cdot 5 \cdot f_5(P_4) + 2 \cdot f_6(P_5) + f_6(P_6)$
$P_8 = (7, 6)(1, 2)(3, 4, 5)$		168	1.4	$2 \cdot f_6(P_6) + 3 \cdot f_6(P_5)$
$P_9 = (8, 7)(1, 2, 3, 4, 5, 6)$	8	1080	1.5	$6 \cdot f_7(P_7)$
$P_{10} = (8, 7, 1)(2, 3, 4, 5, 6)$		1140	1.583	$6 \cdot 5 \cdot f_5(P_4) + 5 \cdot f_7(P_7)$
$P_{11} = (8, 7, 1, 2)(3, 4, 5, 6)$		1104	1.533	$2 \cdot 6 \cdot f_6(P_5) + 4 \cdot f_7(P_7)$
$P_{12} = (8, 7)(1, 2)(3, 4)(5, 6)$		1008	1.4	$6 \cdot f_7(P_8)$

Derivation of Table 1. The formulas given in Table 1 are easily written out using Theorem 2 and Lemma 1. For example, the two terms for $f_7(P_8)$ are generated by i in the cycles $(1, 2)$ and $(3, 4, 5)$. The second term for $f_5(P_4)$ is generated by $i = 2$. When i is 1 or 3 the permutation $P_4\phi_i$ has a single fixed point, namely 4 or 3, and a second application of Theorem 2 produces the first term for $f_5(P_4)$. Since $f(P)$ depends only on the cycle structure of P, there is an alternate formula

$$5 \cdot 4 \cdot f_5(P_3) + 4 \cdot f_6(P_5)$$

for $f_7(P_8)$ corresponding to the permutation $(7, 6, 1)(2, 3)(4, 5)$.

3. Proof of Theorem 1

Suppose $P \in A_n$ has a fixed point, which may be assumed to be n. Then Theorem 2 and (a) of Lemma 1 imply

$$f(P) = (n-1)f(P\pi_n^{-1}), \quad nP = n, \tag{1}$$

and the first part of Theorem 1 is immediate.

Now consider the second part of Theorem 1. Theorem 2, (c) and (d) of Lemma 1, and (1) above imply

$$\begin{aligned} f^+(n) \leq \max\{&(n-2)f^+(n-1), \\ &(n-3)f^+(n-1) + (n-2)(n-3)f^+(n-3), \\ &(n-4)f^+(n-1) + 2(n-2)f^+(n-2)\}, \end{aligned} \tag{2}$$

where $f^+(n)$ is the maximum of $f(P)$ for P in $A_n \cap D_n$. The three cases in (2) reflect three possible values for $|c(n, P)|$, namely, 2, 3, and ≥ 4. The extra terms are introduced via (1) for the same reasons given at the end of Section 2. A tedious expansion of polynomials of degree at most 6 will show that

$$h^+(n) = (n-2)! \prod_{k=4}^{n-2} (1 + 2/k^2)$$

satisfies (2) with reversed inequality for $n \geq 8$. A quick glance at Table 1 shows that

$$f^+(n)/(n-2)! \leq \tfrac{4}{3} h^+(n)/(n-2)! \tag{3}$$

for $5 \leq n \leq 7$. By induction, (3) holds for $5 \leq n$. Numerical methods will show

$$\lim_{n\to\infty} h^+(n)/(n-2)! = 1.739 \cdots < \tfrac{7}{4}.$$

Hence $f(P)/(n-2)! \leq \frac{7}{3}$ for P in $A_n \cap D_n$ as claimed. A similar, but simpler, argument shows

$$f^-(n) \geq h^-(n) = \tfrac{4}{3}(n-2)! \quad \text{for} \quad 5 \leq n.$$

References

[1] E.A. Bertram, Even permutations as a product of two conjugate cycles, J. Combinatorial Theory A 12 (1972) 368–380.
[2] J.L. Brenner and J. Riddell, Noncanonical factorization of a permutation, Amer. Math. Monthly 84 (1977) 39–40.
[3] D.H. Husemoller, Ramified coverings of Riemann surfaces, Duke Math. J. 29 (1962) 167–174. (Proposition 4).
[4] G. Moran, Reflection classes whose cubes cover the alternating group, J. Combinatorial Theory A 21 (1976) 1–19.
[5] O. Ore, Some remarks on commutators, Proc. Amer. Math. Soc. 2 (1951) 307–314.
[6] J. Riordan, An Introduction to Combinatorial Analysis (Wiley, New York, 1958). (Section 3.4).
[7] D. W. Walkup, Matchings in random regular bipartite digraphs, to appear in Discrete Mathematics.
[8] E.M. Wright, For how many edges is a digraph almost certainly Hamiltonian?, Proc. Amer. Math. Soc. 41 (1973) 384–388.